1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 ("DPA"), the Freedom of Information Act 2000 ("FOIA"), the Environmental Information Regulations ("EIR") and the Privacy and Electronic Communications Regulations 2003 ("PECR"). He also deals with complaints under the Re-use of Public Sector Information Regulations 2015 ("RPSI") and the INSPIRE Regulations 2009.

2. He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

3. The Commissioner welcomes the opportunity to respond to the Committee’s inquiry.

4. The term ‘online platforms’ is very broad and the Information Commissioner takes this to include most of the main providers of online services. Different types of service pose different types of challenge – and opportunity. His evidence will try to focus on the broader issues that are common to all or most of them.

5. The DPA and the corresponding European Directive (95/46) don’t define the concept of ‘online platform’ - they focus on the concept of a data controller – a person who decides the purposes for which personal data is used. Most online platforms are likely to be data controllers. The judgment from the Court of Justice (CJEU) in the
Google Spain case, delivered in 2014, found that Google was data controller in respect of its search engine service¹.

6. The use of personal data is increasingly central to the way online platforms operate, particularly in terms of personalisation and monetisation. As online platforms operate across a range of devices there are new opportunities to increase the range and volume of personal data collected, combined and analysed – for example data about location is now routinely collected and used. The link between some online platforms and other connected devices within the ‘internet of things’ will also increase the amount of data available to online platforms – for example, fitness trackers.

7. The Commissioner has recently submitted his response to the Science and Technology Select Committee on the topic of big data². The Information Commissioner recognises the benefits of big data and that data protection should not unnecessarily restrict innovative uses of data but the Commissioner has been clear that big data can’t be seen as a game played by different rules and rules of data protection must apply.

8. The European Commission’s Strategy for the digital single market highlights the importance of concluding the negotiations on the General Data Protection Regulation (GDPR). The Information Commissioner has supported the case for reform of the current European Data Protection Directive, to meet the challenge of upholding data protection rights in a digital economy and information society. The Commissioner has set out his views on the various iterations of the GDPR (Commission, Parliament and Council texts) as the negotiations have progressed³. Enhanced rights for

¹ Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. C-131/12
² Information Commissioner’s submission to the Science and Technology Select Committee on big data
³ ICO paper on proposed Commission text of GDR

ICO blog on European Parliament text of GDPR

15/10/15 Version 1.0 (Final)
data subjects, provisions on accountability and clearer powers for Data Protection Authorities are all positive aspects of the text. However, the Commissioner has warned of over-prescription in certain areas of the text and the importance of it supporting a risk based approach to compliance.

9. He is also supportive of the Commission’s proposal to review the e-Privacy Directive, following the conclusion of the GDPR negotiations, which would include the concept of “electronic communications service”.

10. The Information Commissioner is responsible for regulating data protection and freedom of information law. Many issues that the Committee may wish to consider in terms of the digital single market will fall outside the scope of his competence. For example, the market dominance of some of the major online players is not in itself an issue for the Commissioner. However, this does have implications for consumer choice in terms of how their information is used and for the balance of power between individuals and the organisations that collect their personal data online; this is a data protection matter. The Commissioner has set out some introductory observations and answered some of the specific questions set by the Inquiry.

11. It is important for operators of online platforms to be clear and transparent about the status of the information they use to deliver content and services to their users. The personalisation of content delivery based on browser generated behaviour has become a major feature of many of the online platforms. It is important for the industry to acknowledge more clearly that when they analyse users’ behaviour to deliver personalised content – location-based advertising for example – then they are processing personal data and all the rules of data protection law apply. This has been a contentious issue for many years and some online platform providers have argued that they are only processing ‘pseudonymous personal data’ - and should be subject to light-touch regulation. The Commissioner recognises that different forms of personal identification pose different levels of privacy risk – the relevant law

ICO paper on Council of the EU text of GDPR

15/10/15 Version 1.0 (Final)
and regulatory practice should recognise this. However, users of online platforms need greater clarity as to the rights they enjoy and service providers need greater clarity as to the rules they must follow when processing their users’ personal data.

12. The Information Commissioner is aware that not all of the longstanding rules of data protection can be applied neatly to all the various types of online platform. For example, he has argued that search engines are data controllers and are processing personal data when, for example, they deliver name-based search results. This was also the view of the CJEU in the Google Spain case. The right of data subjects to request links to be de-listed is an important mechanism to allow users to control what happens to information about them online. The Information Commissioner recognises the importance of balancing this right against the right of users to receive information online and this is still an area that online platforms and data authorities are learning to navigate. However, the Commissioner would argue that the implementation of the Google Spain judgment has worked well in practice and many of concerns first raised about the judgment were not realised.

13. Effective application of data protection rules to online platforms will require innovation and a ‘privacy by design’ approach. The Information Commissioner is supportive of different approaches that can deliver data protection compliance more effectively in the digital world, for example innovation delivering better ‘just-in-time’ privacy information, built into the delivery of an online service, rather than reliance on lengthy notices delivered to the user as a single point of interaction.

14. Many online platforms are operated by US companies, often with complex international structures. Some have no physical presence – or ‘establishment’ in data protection terms – within the EU. This means that currently they are not subject to EU law, even though their services may have many EU users and be targeted specifically at them. Other companies may have an HQ in one EU country but with regional offices in other EU countries, for example. The ‘territoriality’ and ‘applicable law’ aspects of data protection law can be complicated to apply in practice. The General Data Protection Regulation seeks to address this problem by making it clear that all companies offering goods and services to EU consumers are subject
to EU law. This is welcome in that it will – in theory – provide better data protection for UK and EU consumers regardless of the territorial aspects of the online platforms whose services they use. In practice though EU data protection rights could be difficult or respect of companies with no EU presence.

15. As online platforms are often offering services to users across the EU there will be an increasing need to address issues of data protection compliance at an EU, rather than national, level. The GDPR anticipates this and contains the concept of a “one stop shop” which would enable a “lead data protection authority” to take measures against a data controller when they are established in more than one member state. This will increase consistency and clarity for online platforms and should support co-ordinated action that can benefit data subjects. The GDPR also proposes that the lead authority would submit proposed measures to the new European Data Protection Board for consideration (the Board will be made up of all the EU Data Protection Authorities). The Information Commissioner has been supportive of the one stop shop concept but has highlighted the risk of too many cases being referred into the process and the need for flexibility to allow authorities to address issues at member state level when it is practical and reasonable to do so.

16. A major requirement of data protection law is transparency in terms of how information is being collected and what it is to be used for. Some online platforms are very complex structures involving a number of different actors. It can be difficult to communicate this to service users and for them to understand how their data is combined and used across a multifunctional platform. Platforms must find more effective means of explaining their complex information systems to ‘ordinary’ service users. This is important as transparency opens the way to the exercise of individuals’ rights, and choice and control over their personal data. Following an investigation by the Information Commissioner, Google recently signed an undertaking\(^4\) to improve its privacy policy, which covers the combination of the data from all its services such search, YouTube and Gmail. The Information Commissioner’s investigation

---

was co-ordinated with a special taskforce made up of a number of other European Data Protection Authorities, within the Article 29 Working Party group of Data Protection Authorities.

17. It is often assumed that young people, for example users of social media sites, do not care about their privacy and that therefore service users can lower their standards in respect of data collection and use. We do not believe this is the case. In fact individuals are managing their privacy choices – for example the way which individuals control access to the various parts of their social media profiles – in relatively sophisticated ways. The popularity of ‘self-destructing’ content services are indicative of individuals’ desire to minimise their ‘cyber-trail’. It is interesting – and welcome - that privacy is also being used as a marketing tool and way of market differentiation.

18. The proposed GDPR contains an article that enables Data Protection Authorities to support privacy seal schemes, as a way of demonstrating data protection compliance. In anticipation of this the Information Commissioner is currently developing a privacy seal programme that will enable data controllers to apply for a seal. Third party scheme operators will apply to the Information Commissioner for an endorsement that will enable them to award the seal. The Commissioner will launch a call for applications later in 2015, with first scheme likely to formally launched sometime in 2016.